Ilyesse El Adaoui

P.108

06/03/2023

Travail à faire :

1.Identifiez les configurations qui présentent des risques pour la sécurité des données.

>Doc 1.2
>Fiche Savoir Technologique 5 (p 119-120)

Les configurations qui représentent des risques pour les données sont le regroupement d'utilisateurs qui donne des privilèges au sein du domaine.
Les comptes doivent donner un accès aux données nécessaires et y accéder par un login et un password.
L'administrateur est le seul à avoir un pouvoir sur le SI, s' il n'est pas bien protégé la sécurité des données de tous les utilisateurs est nul .

2. A partir des différentes informations que vous avez relevées,rédigez une synthèse des bonnes pratiques à adopter.

>Doc 3.4 (p 108-109)
>Fiche Savoir Technologique 6 (p 121)

- Avoir un dossier à son nom pour chaque partenaires pour stocker ses données.
- Contrôle d'accès sur les autorisations des actions faites par l'utilisateur.
- Restreindre et privilégier des droits sur les fichiers des utilisateurs.
- Gestion des droits d'accès au sein du SI (accès à la modification des données qu'aux personnes autorisées).
- Politique de contrôle d'accès de la ressource.

3.Indiquez quel autre problème de sécurité pourrait être provoqué par des privilèges accordés aux utilisateurs.

>Doc 4 (p 110)
>Fiche Savoir Technologique 6 (p 121)

L'utilisateur à le contrôle et les droits sur tous.
Il faudrait limiter les accès aux utilisateurs et contrôler leurs actions.

4.Précisez les préconisations à adopter quant à la segmentation du SI de la MSAP.

>Doc 5
>Fiche Savoir Technologique 5, 6,7 (p 119- 126)

- Les comptes doivent donner un accès aux données nécessaires et y accéder par un login et un password.
- Avoir un dossier à son nom pour chaque partenaires pour stocker ses données.
- Contrôle d'accès sur les autorisations des actions faites par l'utilisateur.
- Restreindre et privilégier des droits sur les fichiers des utilisateurs.
- Gestion des droits d'accès au sein du SI (accès à la modification des données qu'aux personnes autorisées).
- Politique de contrôle d'accès de la ressource.
- Il faudrait limiter les accès aux utilisateurs et contrôler leurs actions.
- Mettre en place un Protocole de communication
- Imposer des règles pour autoriser les communications.